富　谷　市

情報セキュリティポリシー
基本方針

１．１ 版

平成 29 年 5 月 1 日　制定
令和 4 年 3 月 31 日　改定

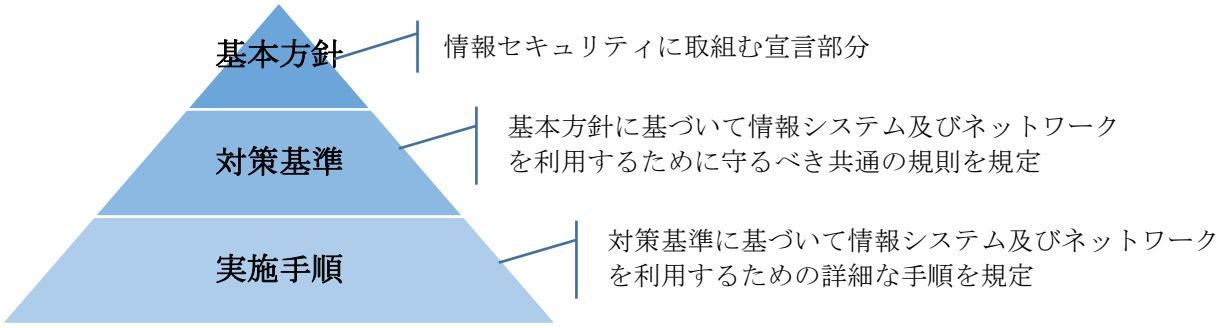
１．情報セキュリティポリシーの構成

情報セキュリティポリシーとは、当市が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめた規則を総称する。情報セキュリティポリシーは、常勤職員、非常勤職員、臨時職員（以下「職員等」という。）及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。

一方、情報セキュリティを取り巻く状況は、技術の進歩や脅威の多様化及び脆弱性の頻出等に伴い急速に変化してきているのが実態である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と、情報資産を取り巻く環境の変化に応じて改編する部分（対策基準）の2階層に分け、それぞれを策定するとともに、職員等が実施する具体的な手順については、情報セキュリティ実施手順として策定（下図参照）し、柔軟かつ迅速な情報セキュリティ対策を行うことを目指すものである。

【情報セキュリティポリシーの構成図】



２．目的

本基本方針は、当市が保有する情報資産の機密性、完全性及び可用性を維持するための対策を整備するために情報セキュリティポリシーを定め、これに従い当市が実施する情報セキュリティ対策について基本的な事項を基本方針として定めることを目的とする。

３．定義

(1) ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(2) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(4) 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

(5) 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(6) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(7) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(8) マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

(9) LGWAN 接続系

LGWANに接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

(10) インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(11) 通信経路の分割

LGWAN接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(12) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

４．対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規程違反、設計・開発関連文書の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3) 地震、落雷、火災等の災害によるサービス及び業務の停止等

(4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

５．適用範囲

(1) 行政機関の範囲

本基本方針が適用される行政機関は、内部部局、各行政委員会、水道事業(以下「部局等」という)とし、各教育機関(学校等)は対象外とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③情報システムの仕様書及びネットワーク図等のシステム関連文書

６．職員等の遵守義務

職員、非常勤職員及び臨時職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

７．情報セキュリティ対策

上記 4.の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制

本市の情報資産について、職員等がそれぞれの責任において率先して情報セキュリティ対策を推進・管理する全庁的な組織体制を確立するとともに、外部委託事業者においても同様の体制確立を要請することとする。

(2) 情報資産の分類と管理

当市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類による重要度に応じた情報セキュリティ対策を行うものとする。

(3) 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(4) 物理的セキュリティ

情報システム及び情報機器を設置する施設への不正な立ち入り、情報資産の破損・破壊・窃用・盗難等から保護するために物理的な対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関する権限や責任を定め、職員等及び外部委託事業者に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発を行う等の人的な対策を講じる。

(6) 技術的セキュリティ

外部及び内部からの不正アクセス、不正プログラム等から適切に保護するため、情報資産へのアクセス制御、コンピュータ及びネットワークの管理・監視等の技術的対策を講じる。

(7) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、システム開発等の外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

(8) 外部サービスの利用

外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

約款による外部サービスを利用する場合には、利用にかかる規程を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

(9) 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

８．情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

９．　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化、外部からの指摘や苦情等に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

１０．情報セキュリティ対策基準の策定

上記 7. 8.及び 9.に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。当該基準は、情報セキュリティ対策を行う上での基本的な要件を明記するものである。

１１．情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守し、個々の情報資産の脅威と重要性に基づく情報セキュリティ対策を実施するための具体的な手順を情報セキュリティ実施手順として策定することとする。

なお、情報セキュリティ実施手順は、公にすることにより当市の行政運営に重大な支障を及ぼす恐れがあることから非公開とする。